FUTURE OF PRIVACY FORUM
1400 eye street nw, ste 450 | washington, dc 20005 • 202-768-8950 • fpf.org

September 12, 2016

Re: Protecting the Privacy of Broadband and Other Telecommunications Services, WC Docket No. 16-106

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Dear Ms. Dortch:

On September 8, Khaled El Emam of Privacy Analytics and I met with Matt Del Nero, Lisa Hone, David Brody, E. Alex Espinoza, Melissa Kirkel, Heather Hendrickson, and Sherwin Siy of the Wireline Competition Bureau, Scott Jordan, the Chief Technology Officer, Jonathan Mayer Chief Technology Officer of the Enforcement Bureau, and Paul de Sa of the Office of Strategic Planning. We discussed the ways in which the Commission could ensure that its proposed broadband privacy rules align with generally accepted privacy regimes around the world, including that of the FTC. In particular, we recommended that any rules the Commission adopts should allow for approaches to de-identification other than aggregation, and should distinguish between sensitive and non-sensitive data.

With respect to de-identification, we discussed the benefits of de-identifying data, and described the various approaches other than aggregation to de-identifying data that preserve the utility of such data while protecting consumer privacy by minimizing the risk that data will be de-identified.[1] For example, we described how, in the health-care context, a process-based approach to de-identification, using expert review of the approach taken, has been effective. We also noted that in privacy regimes that establish high de-identification thresholds, it has been necessary to provide exceptions allowing uses of data for research and for analysis. In contrast, a

---

* The Future of Privacy Forum (FPF) is a not for profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies.

† The views herein do not necessarily reflect those of our members or our Advisory Board.

[1] The approaches to de-identification we described are consistent with the high-level standards set by the Federal Trade Commission and consistent with NIST Special Publication 800-188. Those high-level standards allow for implementation using an approach that relies on standards that are well accepted in the disclosure control community.

risk-based standard for achieving de-identification that preserves the utility of data would enable uses such as research and product development without sacrificing consumer privacy.

We also explained why the widely reported examples of data being re-identified actually do not support an inflexible policy towards de-identification. Specifically, these examples involved data that had not been properly de-identified or had not been de-identified at all. In contrast to these examples, there is significant evidence demonstrating that properly de-identified data cannot easily be re-identified, so proper de-identification, along with appropriate controls, is a tool that permits data to be used in a manner that protects privacy.[2]

With respect to the distinction between sensitive and non-sensitive information, we discussed briefly the fact that, generally, privacy laws around the world distinguish between the two, and require higher levels of notice and consent for the disclosure of sensitive data. For example:

- The new EU General Data Protection Regulation, which will soon govern all information processing in Europe, describes 'special categories of data' that may not be processed unless the data subject has given explicit consent….for one or more specified purposes…." or under certain exigent circumstances.[3].

- PIPEDA, the privacy regime for Canada, determines the level of consent required for use and disclosure of data on its sensitivity.[4]

- In its 2012 Privacy Report, the Federal Trade Commission also noted that "[i]n instances where data is more sensitive or may affect benefits, more individualized notice, access and correction rights may be warranted."[5]

- Generalizing from this principle, the Administration's Consumer Privacy Bill of Rights states that "individuals should be provided with "reasonable means to control the processing of personal data about them **in proportion to the privacy risk** to the individual," with privacy risk defined as the potential for the data to cause emotional distress, or physical, financial, professional or other harm to the individual."[6]

---

[2] See Elliot, Mackey, O'Hara and Tudor, "The Anonymisation Decision-Making Framework" (2016) (offering guidance regarding the reasonable de-identification of data with a foreword and endorsement of the guidance by Elizabeth Denham, UK Information Commissioner); C. Tudor, "Intruder Testing on the 2011 UK Census: Providing Practical Evidence for Disclosure Protection," Journal of Privacy and Confidentiality, vol. 5, no. 2, Aug. 2013 (finding that after recruiting volunteers to attack a data set, "it is very difficult to re-identify respondents correctly in the 2011 UK Census […] Even given that the claims that were made about people the intruder would expect to know reasonably well, i.e., family, themselves, or a neighbour, the percentage of correct claims was still surprisingly low.").

[3] Regulation (EU) 2016/679, General Data Protection Regulation (GDPR), Art.9.

[4] Personal Information Protection and Electronic Documents Act (PIPEDA), S.C. 2000, c. 5 (last amended 2016-06-23), Principle 4.3.5.

[5] FEDERAL TRADE COMMISSION, REPORT: PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (March 2012) at 67.

[6] THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (February 23, 2012) at 2, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

While different laws, and even different self-regulatory bodies, articulate different nuances in defining "sensitive" data, the core principles that distinguish sensitive from non-sensitive information are remarkably similar. Rules developed to prevent consumer harm generally identify types of information that cannot be used or disclosed without a very high level of consent based on the risk of harm that unexpected disclosure of these types of data present in a particular society.

Though some commenters who have dismissed the sensitivity-based framework because they assert that it requires more invasive inspection of data to implement, we described uses of data that do not involve collection of sensitive data at all, or do not use data beyond what is already collected for other purposes, or where categories are created that ensure that only non-sensitive data is used.

We include as attachments a copy of the presentation that was used to guide the discussion and a paper authored by Dr. El Emam in response to the Commission's proposed rules. The paper is intended to compare the Commission's proposal with other approaches to de-identification regulations and methodologies, and to propose an alternative approach that will allow for the beneficial uses of de-identified data while reducing privacy risks for consumers.

Please direct any questions to the undersigned.

Sincerely,

/s/ Jules Polonetsky
Jules Polonetsky
Chief Executive Officer
Future of Privacy Forum